

1 File Descriptions

This Chapter provides descriptions of the following F-PROT Professional files: SETUP.EXE, Program Files, F-PROTW.CFG, User Profile Files, F-PROTW.INI, AUTOINST.INI, UPDATE.INI, FPW-PREF.INI, Search String Files, Task Files, the Log File, Task Result Files (Reports), Infected And Suspected Files, Message Files, Bulletin Files, COMM.INF, and TMP.~NF.

1.1 SETUP.EXE

The installation program, SETUP.EXE, is used for installing F-PROT Professional on workstations and/or on the server.

1.2 Program Files

F-PROT Professional for Windows consists, in fact, of two separate programs, Launcher and Main Program, each of which has its own functions. When a user starts F-PROT Professional, the **Launcher** is executed first. The Launcher performs certain preliminary tasks and then starts the **Main Program**.

Launcher

When F-PROT is run in user mode, the Launcher (F-PROTW.EXE, F-PROTNT.EXE, or F-PROT95.EXE, depending on the operating environment) checks whether a new version of the program has become available. If a new version has appeared in the shared UPDATE directory, Launcher reads the Update Preference to find out whether the program should be updated without notifying the user.

If the user's confirmation is required before updating, Launcher requests it. Otherwise, it proceeds directly to copying the new program version to the local

F-PROT Professional for Windows root directory. Having done this, it executes the Main Program

If F-PROT Professional is run in administration mode, Launcher skips the version check and immediately starts the Main Program.

Main Program

The Main Program (FPWM.DLL, FPWM32.DLL) is the visible part of the application. When started, it executes the Memory Check at the beginning of its first scan. Then, if in user mode, it checks the shared disk for new tasks, user-defined signatures, and bulletins. It also checks the local INFECT, SUSPECT and REPORT directories for reports and infected and suspected files that should be sent to the administrator. If it finds any such items, it copies them from or to the shared disk.

Having completed these preliminary tasks, the Main Program informs the user of new bulletins and continues its normal routine, periodically checking the shared disk for new tasks, signatures and bulletins.

When executed in administration mode, the Main Program first checks the shared disk directories MESSAGES, INFECTED, SUSPECT and REPORT for user messages, infected and suspected files, and reports from other workstations. It then informs the administrator of its findings. Afterwards, it periodically checks the shared disk for messages, reports, and infected or suspected files.

1.3 F-PROTW.CFG

F-PROTW.CFG is the F-PROT Professional for Windows system file. It contains the User Profile and other information needed for the program's successful execution. F-PROTW.CFG is located not in the F-PROT root directory, but in the Windows root directory. F-PROTW.CFG is encrypted.

1.4 User Profile Files

A User Profile file contains the user Preferences. At the same time, the User Profile file can also act as the F-PROT Professional system file, F-PROTW.CFG. The administrator can create and save several different User Profiles and move the User Profile files onto the shared disk to be installed directly from the network.

On a user workstation, a User Profile file acts as the system file, F-PROTW.CFG. Therefore, all User Profile files must be named F-PROTW.CFG before the programs are installed onto workstations. Otherwise F-PROT will not recognize these files.

1.5 F-PROTW.INI

NOTE This section applies only to Windows 3.1x version.

F-PROTW.INI is the definition file, used by both F-PROT Professional for Windows 3.1 and F-PROT Gatekeeper operating under Windows 3.1.

One use of F-PROTW.INI is to define the memory areas which are not to be scanned for viruses. Some exotic display drivers are incompatible with a memory scan. If your system uses such a driver, the latter may cause Windows to stop responding during a memory scan. Should this occur, follow the instructions below:

- Always save your work in other Windows applications before running the memory scan tests. If Windows stops responding, there is no way to continue the Windows session and it will be necessary to re-start the computer.
- Create the F-PROTW.INI file in the Windows directory. If the F-PROTW.INI file already exists, simply edit the existing file To determine which memory areas should be skipped, enter "ShowSegmentNumber=1" into the [MemoryScan] section of F-PROTW.INI, for example:
- [MemoryScan]
ShowSegmentNumber=1
- This will make F-PROT Gatekeeper's memory scanner display the number of scanned memory segments rather than the percentage completed in the progress indicator window.
- Restart Windows to see the memory being scanned.
- When Windows stops responding, write down the segment number shown in the progress window. For example, if the window shows "Scanning Segment 1a", the segment number is "1a". After rebooting, write "AreaStatusXX=1" (in which XX stands for the segment number) into the [MemoryScan] section of F-PROTW.INI.

For example:

```
[MemoryScan]
ShowSegmentNumber=1
AreaStatus1a=1
```

- Then run the memory scan again. If Windows stops responding again (this time in another segment), simply write another "AreaStatus" line to F-PROTW.INI. It is very unlikely that Windows will stop responding more than once or twice. Finally, comment out or remove the "ShowSegmentNumber=1" entry from F-PROTW.INI or set the value to zero.

Remember, the memory scan hanging problem is caused by incompatibilities with certain video drivers. Therefore, if you change your video driver, try removing the "AreaStatusXX=1" entries and running the memory scan again to see what happens.

1.6 AUTOINST.INI

AUTOINST.INI is a parameter file for AUTOINST, the utility program for F-PROT automatic installation or updating on workstations logged on to a network. The workstations normally call a login batch script (LOGIN.BAT, for instance) when they log on to the network. The login batch script is modified to invoke AUTOINST. AUTOINST then performs the installation according to the instructions it finds in its parameter file AUTOINST.INI.

The program files and configuration files are placed on a network drive by the administrator. AUTOINST copies them to the local drive and makes necessary changes to the user's WIN.INI, SYSTEM.INI files and/or makes the necessary registrations. AUTOINST also handles updating and uninstallation, and can be used for changing configuration (preferences) of workstations throughout the network. Refer to Chapter 13, "AUTOINST," to learn how to fine-tune AUTOINST.INI using a text editor.

1.7 UPDATE.INI

UPDATE.INI is an ASCII file which AUTOINST uses to determine whether or not to update (copy) files to the destination directory. This file is also used by F-PROT Professional for automatic updating by F-PROTNT.EXE, F-PROTW.EXE, or F-PROT95.EXE, depending on the platform.

AUTOINST opens the UPDATE.INI file located in the source directory and the other UPDATE.INI file located in the destination directory to compare the file dates. If

either the source or the destination directory does not contain UPDATE.INI, or if the date strings of the two files are different, AUTOINST copies the files. If the dates are identical, the files are not copied.

Note that UPDATE.INI affects only the copying of program files. It has no effect on whether the configuration files are copied, or edited on the local drive according to the settings specified in AUTOINST.INI.

Example of UPDATE.INI:

```
[LastChange]
LastChange=95-03-15
```

Note that when the program files are copied, UPDATE.INI is also copied. Therefore, the two copies will be identical after the first run, and program files are not copied upon subsequent runs. Be sure to change the date in UPDATE.INI before sending an update.

1.8 FPW-PREF.INI

F-PROT Professional allows to update files, such as VIRSTOP.EXE (a TSR in the DOS version), from the network server to local workstations. When F-PROT Professional starts, it checks the file FPW-PREF.INI. Copy this file to the directory which contains F-PROTW.EXE.

FPW-PREF.INI should contain lines like the following:

```
[Update]
Source=V:\MASTER\F-PROT
Destination=C:\F-PROT
```

The FPW-PREF.INI file causes F-PROT Professional to update files from the server directory V:\MASTER\F-PROT to the local directory C:\F-PROT each time it starts up.

For example, to update the file VIRSTOP.EXE (a TSR in the DOS version) on all the workstations, the administrator only needs to update VIRSTOP in the master directory on the server. Then F-PROT Professional will make sure that all the workstations run an up-to-date copy of VIRSTOP.

1.9 Search String Files

The Search String Files contain the search strings F-PROT uses for detecting viruses. F-PROT Professional has its own search string database.

F-PROT Professional Search Strings

The F-PROT virus search strings are stored in the file SIGN.DEF. This file is specifically encrypted, so that it can be accessed only by F-PROT.

1.10 Task Files

Parameters of each F-PROT task parameters are are stored in an encrypted task file, located in the local TASKS directory. When F-PROT is started, it reads all the task files and displays the corresponding tasks on the task list.

Default Tasks

F-PROT Professional contains one default task, which is hard-coded into the program and cannot be deleted. When F-PROT is installed, it creates the task file for the default task and displays the task as Default task on the task list. Although the default task cannot be deleted, its parameters can be modified normally.

Other pre-configured tasks may also be included in the program. Such tasks are stored in normal task files, and do not differ from ordinary, user-defined tasks.

User-Defined Tasks

User-defined task files have the extension FPT, which means F-PROT Task. The file name is generated from the first 8 letters of the task name. For example: "Scan Network File Servers with Secure Scan" becomes "SCANNETW.FPT". In case of a duplicate name, F-PROT replaces the last four letters of the task file name with a four-digit number. For example: "SCAN0001.FPT", "SCAN0002.FPT".

Administrator's Tasks

The tasks distributed by the administrator are named in the same way as the user tasks, except that the file extension is FPA, F-PROT Administrator's Task.

1.11 The Log File

The log file, F-PROTW.LOG, contains one line per executed task. A log entry consists of the task name, its execution time and result.

The log file is stored at the LOCAL directory.

1.12 Task Result Files (Reports)

A results file (report) contains the results of one or several tasks. If the **Append** option is selected in the **Reporting** Preference, the file contains the results of several consequent scans, otherwise it contains the results of only one task.

The result file name is the same as the corresponding task file name, but its extension is FPR (F-PROT Result File), for example: SCANNETW.FPR. Results files are in binary format and cannot be browsed with a text editor. On local workstations, the results files are stored in the REPORTS directory. On administration workstation, reports from user workstations are stored in the REPUSER directory.

The reports can be inspected while inside the program. Warnings of viruses are shown in red. Headings are in larger font sizes.

A results file has the following elements:

- The heading, which states the task name and execution time. The user name and the workstation name are given below.
- The brief description of the task parameters.
- The summary of results. For example:
'Scanned 1 disk(s), 14 file(s). No viruses found.', or

'Scanned 1 disk(s), 14 file(s). Alert! Found 2 virus(es) in 30 file(s). Disinfected 0 file(s).'

- If infections have been found, the infected files are arranged under entries that state the infecting virus. For example:

'Found the Jerusalem virus in

C:\APPS\BIN\QEDIT.EXE

C:\DOS\FORMAT.COM

'Found the Vienna virus in

C:\COMMAND.COM

Double-clicking on the infected file name opens a window where the file is described in more detail. Double-clicking on the infecting virus name displays the description of the virus.

1.13 Infected And Suspected Files

Infected and suspected files are the files which have a confirmed or suspected virus infection. When such files are sent from local workstations to administrator, they are renamed to prevent spreading of infection through accidental execution of the files.

The substitute name for an infected file is formed by concatenating the letters INF and the current five-digit infected file count number, which may contain leading zeros. The renamed files have the extension VIR, for example: INF00015.VIR

The substitute name of a suspected file is similarly formed by concatenating the letters SUS and the running five-digit suspected file count number, which can include leading zeros, for example: SUS00015.VIR

When infected and suspected files are sent to administrator, each of them is accompanied by the information file, which contains the name of the infecting virus, the local workstation's name, the name of the original file and its directory path. The information files have the extension INF. Their names are formed by concatenating the letters INF and the running five-digit count number, which may include leading zeros, for example: INF00015.INF

1.14 Message Files

Message files are simple text files sent from users to the administrator. Besides the actual message, a message file contains, in its first three lines, the subject of the message, the ID of the sending workstation, and the sender's user name.

Message files have the extension TXT. Their names are concatenations of the letters MSG and the running five-digit message count number, which may include leading zeros, for example: MSG00130.TXT.

1.15 Bulletin Files

The Bulletin File

Any file, regardless of its format, can serve as a bulletin file, as long as both its sender and recipient possess the application needed to read the file. In practice, this means the text editor or other application with which the bulletin file was created.

The INF File

Each bulletin is accompanied by the separate file having the extension INF. The INF file contains the name of the bulletin, the name of the application used to create the bulletin, and the name of the bulletin file. When a bulletin is copied from the shared BULLETIN directory to a local workstation, this information is incorporated into the local F-PROTW.CFG.

The name of each INF file is the concatenation of the letters BUL and the running five-digit bulletin count number, which may include leading zeros, for example: BUL00015.INF.

1.16 COMM.INF

The COMM.INF file tracks all tasks, messages, bulletins, search strings, reports, and infected files sent through the network. COMM.INF is located on the shared disk,

and is accessed periodically by the local F-PROT programs which check for new tasks, bulletins, messages, and reports. The COMM.INF file is encrypted.

1.17 TMP.~NF

Every time F-Agent or F-PROT running on a workstation starts reading the shared communications directory, the semaphore file named TMP.~NF is created in the communications directory, unless it already exists. As long as the semaphore file exists, F-Agent or F-PROT from no other workstation can access the communications directory. After reading the needed information, F-PROT deletes the TMP.~NF, so that other workstations are able to access the communications files.